



FortiOS - Release Notes

Version 5.6.7

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



November 27, 2018

FortiOS 5.6.7 Release Notes

01-567-524011-20181127

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported models	5
VXLAN supported models	6
Special Notices	7
Built-in certificate	7
FortiGate and FortiWiFi-92D hardware limitation	7
FG-900D and FG-1000D	7
FortiGate-VM 5.6 for VMware ESXi	8
FortiClient profile changes	8
Use of dedicated management interfaces (mgmt1 and mgmt2)	8
FortiExtender support	8
Using ssh-dss algorithm to log in to FortiGate	8
Using FortiAnalyzer units running older versions	8
Upgrade Information	9
Upgrading to FortiOS 5.6.7	9
Security Fabric upgrade	9
FortiClient profiles	10
FortiGate-VM 5.6 for VMware ESXi	10
Downgrading to previous firmware versions	10
Amazon AWS enhanced networking compatibility issue	11
FortiGate VM firmware	11
Firmware image checksums	12
Product Integration and Support	13
FortiOS 5.6.7 support	13
Language support	15
SSL VPN support	15
SSL VPN standalone client	15
SSL VPN web mode	16
SSL VPN host compatibility list	16
Resolved Issues	18
Known Issues	24
Limitations	27
Citrix XenServer limitations	27
Open source XenServer limitations	27

Change Log

Date	Change Description
2018-11-27	Initial release.

Introduction

This document provides the following information for FortiOS 5.6.7 build 1653:

- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Limitations](#)

For FortiOS documentation, see the [Fortinet Document Library](#).

Supported models

FortiOS 5.6.7 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001C, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30D, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-30D-POE, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60E-DSL, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-SVM, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 5.6.7 images are delivered upon request and are not available on the customer support firmware download page.

VXLAN supported models

The following models support VXLAN.

FortiGate	FG-30E, FG-30E-MI, FG-30E-MN, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DLS, FG-60E-MC, FG-60E-MI, FG-60E-POE, FG-60EV, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-DSL, FWF-60E-MC, FWF-60E-MI, FWF-60EV, FWF-61E
FortiGate Rugged	FGR-30D, FGR-30D-A, FGR-35D
FortiGate VM	FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-NPU, FG-VM64-OPC, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN

Special Notices

Built-in certificate

New FortiGate and FortiWiFi D-series and above are shipped with a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate and FortiWiFi-92D hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
  set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result.

FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.7, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

FortiClient profile changes

With introduction of the Fortinet Security Fabric, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

The FortiClient profile on FortiGate is for FortiClient features related to compliance, such as Antivirus, Web Filter, Vulnerability Scan, and Application Firewall. You may set the *Non-Compliance Action* setting to *Block* or *Warn*. FortiClient users can change their features locally to meet the FortiGate compliance criteria. You can also use FortiClient EMS to centrally provision endpoints. The EMS also includes support for additional features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

FortiExtender support

Due to OpenSSL updates, FortiOS 5.6.7 cannot manage FortiExtender 3.2.0 or earlier. If you run FortiOS 5.6.7 with FortiExtender, you must use a newer version of FortiExtender such as 3.2.1 or later.

Using ssh-dss algorithm to log in to FortiGate

In version 5.4.5 and later, using `ssh-dss` algorithm to log in to FortiGate via SSH is no longer supported.

Using FortiAnalyzer units running older versions

When using FortiOS 5.6.7 with FortiAnalyzer units running 5.6.5 or lower, FortiAnalyzer might report increased bandwidth and session counts if there are sessions that last longer than two minutes.

For accurate bandwidth and session counts, upgrade the FortiAnalyzer unit to 5.6.6 or higher, or 6.0.2 or higher.

Upgrade Information

Upgrading to FortiOS 5.6.7

Supported upgrade path information is available on the [Fortinet Customer Service & Support site](#).

To view supported upgrade path information:

1. Go to <https://support.fortinet.com>.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
 - *Current Product*
 - *Current FortiOS Version*
 - *Upgrade To FortiOS Version*
5. Click *Go*.



If you are upgrading from version 5.6.2, this caution does not apply.

Before upgrading, ensure that port 4433 is not used for `admin-port` or `admin-sport` (in `config system global`), or for `SSL VPN` (in `config vpn ssl settings`).

If you are using port 4433, you must change `admin-port`, `admin-sport`, or the `SSL VPN` port to another port number before upgrading.



After upgrading, if FortiLink mode is enabled, you must manually create an explicit firewall policy to allow RADIUS traffic for 802.1x authentication from the FortiSwitch (such as from the FortiLink interface) to the RADIUS server through the FortiGate.

Security Fabric upgrade

FortiOS 5.6.7 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 5.6.1
- FortiClient 5.6.0
- FortiClient EMS 1.2.2
- FortiAP 5.4.2 and later
- FortiSwitch 3.6.2 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

Before upgrading any product, you must read the *FortiOS Security Fabric Upgrade Guide*.

FortiClient profiles

After upgrading from FortiOS 5.4.0 to 5.4.1 and later, your FortiClient profiles will be changed to remove a number of options that are no longer supported. After upgrading, review your FortiClient profiles to make sure they are configured appropriately for your requirements and either modify them if required or create new ones.

The following FortiClient Profile features are no longer supported by FortiOS 5.4.1 and later:

- Advanced FortiClient profiles (XML configuration).
- Advanced configuration, such as configuring CA certificates, unregister option, FortiManager updates, dashboard Banner, client-based logging when on-net, and Single Sign-on Mobility Agent.
- VPN provisioning.
- Advanced AntiVirus settings, such as Scheduled Scan, Scan with FortiSandbox, and Excluded Paths.
- Client-side web filtering when on-net.
- iOS and Android configuration by using the FortiOS GUI.

With FortiOS 5.6.7, endpoints in the Security Fabric require FortiClient 5.6.0. You can use FortiClient 5.4.3 for VPN (IPsec VPN, or SSL VPN) connections to FortiOS 5.6.2, but not for Security Fabric functions.



It is recommended that you use FortiClient Enterprise Management Server (EMS) for detailed Endpoint deployment and provisioning.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.7, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles

If you have long VDOM names, you must shorten the long VDOM names (maximum 11 characters) before downgrading:

1. Back up your configuration.
2. In the backup configuration, replace all long VDOM names with its corresponding short VDOM name.
For example, replace `edit <long_vdom_name>/<short_name>` with `edit <short_name>/<short_name>`.
3. Restore the configuration.
4. Perform the downgrade.

Amazon AWS enhanced networking compatibility issue

With this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.6.7 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 5.6.7 to older versions, running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums


The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.6.7 support

The following table lists 5.6.7 product integration and support information:

Web Browsers	<ul style="list-style-type: none">• Microsoft Edge 38• Mozilla Firefox version 54• Google Chrome version 59• Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	<ul style="list-style-type: none">• Microsoft Edge 40• Microsoft Internet Explorer version 11• Mozilla Firefox version 53• Google Chrome version 58• Apple Safari version 10 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Security Fabric upgrade on page 9 . For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Security Fabric upgrade on page 9 . For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient Microsoft Windows	See important compatibility information in Security Fabric upgrade on page 9 . <ul style="list-style-type: none">• 5.6.1 If FortiClient is managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.
FortiClient Mac OS X	See important compatibility information in Security Fabric upgrade on page 9 . <ul style="list-style-type: none">• 5.6.0 If FortiClient is managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.
FortiClient iOS	<ul style="list-style-type: none">• 5.4.3 and later
FortiClient Android and FortiClient VPN Android	<ul style="list-style-type: none">• 5.4.1 and later

FortiAP	<ul style="list-style-type: none"> • 5.4.2 and later • 5.6.0
FortiAP-S	<ul style="list-style-type: none"> • 5.4.3 and later • 5.6.0
FortiSwitch OS (FortiLink support)	<ul style="list-style-type: none"> • 3.6.2 and later
FortiController	<ul style="list-style-type: none"> • 5.2.5 and later <p>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C.</p>
FortiSandbox	<ul style="list-style-type: none"> • 2.3.3 and later
Fortinet Single Sign-On (FSSO)	<ul style="list-style-type: none"> • 5.0 build 0272 and later (needed for FSSO agent support OU in group filters) <ul style="list-style-type: none"> • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2008 (32-bit and 64-bit) • Windows Server 2008 R2 64-bit • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Novell eDirectory 8.8 <p>FSSO does not currently support IPv6.</p>
FortiExtender	<ul style="list-style-type: none"> • 3.2.1 and later <p>See FortiExtender support on page 8.</p>
AV Engine	5.00361
IPS Engine	3.00539
Virtualization Environments	
Citrix	<ul style="list-style-type: none"> • XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	<ul style="list-style-type: none"> • RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	<ul style="list-style-type: none"> • Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	<ul style="list-style-type: none"> • XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	<ul style="list-style-type: none"> • ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
<div>  <p>FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.</p> </div>	

VM Series - SR-IOV

The following NIC chipset cards are supported:

- Intel 82599
- Intel X540
- Intel X710/XL710

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	2336. Download from the Fortinet Developer Network https://fndn.fortinet.net .
Linux Ubuntu 16.04 (32-bit & 64-bit)	

Other operating systems may function correctly, but are not supported by Fortinet.



SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11
Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Mozilla Firefox version 54
	Google Chrome version 59
Microsoft Windows 10 (64-bit)	Microsoft Edge
	Microsoft Internet Explorer version 11
	Mozilla Firefox version 54
	Google Chrome version 59
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
Mac OS 10.11.1	Apple Safari version 9
	Mozilla Firefox version 54
	Google Chrome version 59
iOS	Apple Safari
	Mozilla Firefox
	Google Chrome
Android	Mozilla Firefox
	Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

It is recommended to verify the accuracy of the GUID for the software you are using for SSL VPN host check. The following Knowledge Base article at <http://kb.fortinet.com/> describes how to identify the GUID for antivirus and firewall products: [How to add non listed 3rd Party AntiVirus and Firewall product to the FortiGate SSL VPN Host check.](#)

After verifying GUIDs, you can update GUIDs in FortiOS using this command:

```
config vpn ssl web host-check-software
```


Following is an example of how to update the GUID for AVG Internet Security 2017 on Windows 7 and Windows 10 by using the FortiOS CLI.



The GUIDs in this example are only for AVG Internet Security 2017 on Windows 7 and Windows 10. The GUIDs might be different for other versions of the software and other operation systems.

To update GUIDs in FortiOS:

1. Use the `config vpn ssl web host-check-software` command to edit the `AVG-Internet-Security-AV` variable to set the following GUID for AVG Internet Security 2017:
4D41356F-32AD-7C42-C820-63775EE4F413.
2. Edit the `AVG-Internet-Security-FW` variable to set the following GUID:
757AB44A-78C2-7D1A-E37F-CA42A037B368.

Resolved Issues

The following issues have been fixed in version 5.6.7. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Antivirus

Bug ID	Description
502138	AV full scan mode causes traffic to fail.

Authentication

Bug ID	Description
453095	Mobile FortiTokens not assignable VDOM in vcluster on slave unit.
473118	Fnbamd crashes after upgrading <code>ca_bundle</code> file.
515226	FortiGate keeps sending accounting packet to RADIUS server for user that is no longer authenticated.

Data Leak Prevention

Bug ID	Description
454103	Certain PDF files being blocked when DLP filter set to block bat file.

Explicit Proxy

Bug ID	Description
491118	Kerberos users unable to access internet.
496294	SNMP value returned OID of <code>fgExplicitProxyMemUsage</code> and <code>fgExplicitProxyUpTime</code> is always 0.
506654	High memory usage on WAD.
509876	Web proxy internet service as <code>dst</code> address cannot work for some IP address range overlap cases.
509994	Web site denied due to certificate error (revoked) only in <code>Proxy_policy</code> and deep inspection profile.
512294	WAD should not keep buffer data if the server's response broke the HTTP protocol.
513667	WAD crash when a callback is triggered during closing procedure.
514426	Explicit proxy cannot catch Microsoft Outlook after FFDB update.

Bug ID	Description
515327	WAD returns '502 Bad Gateway' if the server disconnects without data received.

Firewall

Bug ID	Description
390422	When a firewall address group is used in firewall policy, a wildcard FQDN address should not be allowed to be added into the firewall address group as a member.
511261	RSH connection disconnects when we have multiple commands executed via script and we can see the message <code>no session matched</code> .
514187	VIP ping healthchecks fail with high number of real servers.

GeoIP

Bug ID	Description
465122	GeoIP database mismatch on cluster after every new database release.

GUI

Bug ID	Description
473140	Cannot paste a script or any character in the GUI CLI console.
503867	In GUI, some certificates break the Certificate page.
508596	GUI Dashboard > Interface Bandwidth widget cannot be added for GRE tunnel interfaces.
511776	Once user has assigned token other tokens not listed in pull down menu.
515022	FortiGate and FSA has right connectivity, but Test Connectivity on GUI interface is showing <code>Unreachable</code> or <code>not Authorized</code> .

HA

Bug ID	Description
445214	Slave in AP cluster memory/CPU spike as a result of DHCP/HA sync issue.
485340	Cluster Uptime: -141 days -20:-31:-50.
501147	Moving VDOM to virtual cluster from GUI causes cluster to go out of sync.
510585	HA does not recognize proper ping-server status, hence does not failover when ping-server is down.
510660	Upgrade to build 3574 fails for HA cluster.

Bug ID	Description
511522	HA uninterruptible upgrade from 9790 to 3558 fails.
512383	local-in-policy for ha-mgmt-int doesn't work after reboot.
516779	Confsync cannot work with three members when encryption is enabled.

IPS

Bug ID	Description
465134	SYN proxy still active when syn rate goes below configured threshold or is disabled.
469608	ICMP packets dropped during FortiGate update.
476219	Delay for BFD in IPinIP traffic hitting policy with IPS while IPsec calculates a new key.
497602	After upgrading, sniffer packet on any interface causes drops on kernel and traffic impact. DoS policies used.

IPsec VPN

Bug ID	Description
463441	NAT -T broken with AWS and FortiGate.
481720	Using transparent mode and policy base VPN, about 4 ICMP packets which exceed over MTU 1375 byte are dropped.
515375	VPN goes down randomly, also affects remote sites dialup.

Log & Report

Bug ID	Description
436037	Application logs set the SRC interface and DST interface in reverse.
467367	app-ctrl logs show policyid=0 sessionid=0 and no srcintf and dstintf field.
475694	log rate widget: fortianalyzer log rate is always 0 when no disk log enabled.
500972	Wrong log for FortiGuard block page.
503897	Fortigate-501E units generating logs only for five minutes after rebooting the unit, then do not generate any more logs.
505393	Quad File Dropped Reason forticloud-daily-quota-exceeded.

NPI

Bug ID	Description
462178	Front panel <i>SPEED</i> LED is flashing green when transmitting and receiving data. Affected models: FG-60D, FG-60E, FG-80E, FG-90D, and FG-500D. Affected versions: 5.6, 6.0, and 6.2.

Proxy and WebProxy

Bug ID	Description
454185	Specific application does not work when deep inspection is enabled.
506995	FG-1200D WAD crashing 5.6.5 (WAD MAPI).
512930	WAD crash with signal 11.
513270	Certificate error with SSL deep inspection.
513663	FG-3200D running FOS 5.6.5 – WAD crashing frequently.

Router

Bug ID	Description
476805	FortiGate delays to send keepalive which causes neighbor's hold down timer to expire and reset the BGP neighborship
481731	Router access-list prefix 0.0.0.0/0 is replaced with any after reboot
499100	SD-WAN with IPPool not respecting associated interface if one of the links has a dynamic IP.
500432	IGMP multicast joins taking very long time and uses high NSM CPU utilization.
504164	OSPF - LSA checksum error.
505467	For some OSPFv3 intra-area routes, the next-hop link-local address is not displayed.
507187	BGP Configuration incrementally adding <code>set-aspath</code> attribute with every BGP update.
511203	When using policy route for IPv6, NAT64 does not work.
514410	The BGP default gateway advertised doesn't work after the upgrade without being manually reset.
514851	BGP default route origination doesn't work.
518929	SNMP, OSPF MIB ospfIfState value when designated router is not correct.

SSL VPN

Bug ID	Description
477231	Unable to log in to VMware vSphere vCenter 6.5 through SSL VPN web portal.
477529	SSL VPN web mode IE11 always gets block when host-check is enabled for <code>skip-check-for-unsupported-browser</code> .
493772	Some URLs in SSL VPN return HTTP404.
507068	Internal server page does not display in SSL VPN web-mode; displays OK in tunnel mode.
507242	Internal web site not working through SSL VPN web mode.
511107	For RADIUS with 2FA and password renewal enabled, password change fails due to unexpected state AVP + GUI bug.

System

Bug ID	Description
471191	Improve CLI help text for config system NP6 session-timeout options.
474612	SNAT is using low ports below 1023.
491090	FortiGuard service is unavailable since upgrading to 5.6.3.
503725	NP6 affecting all user traffic when enable on policy.
505522	Intermittent failure of DHCP address assignment.
505715	DHCP lease new IP to same EFTPOS S800 device causes DHCP lease exhausted.
506030	SLBC cluster never in-sync after policy push.
507447	FortiGate 300E is bridging OSPF packets during boot phase.
510200	FortiGate DNS configuration doesn't allow single-word domain names.
510419	HTTP link-monitor - response parser is case-sensitive (Content-Length header).
510737	Users are not able to pull DHCP addresses from FGT.
512963	vdom-properties firewall-address discrepancies.
513156	Packet loss on startup when interfaces are in bypass mode (2500E).
513339	Finisar FCLF8521p2BTL (FG-TRAN-GC) and (FS-TRAN-GC) FCLF8522P2BTL Transceivers not detected by FortiOS.
513671	File descriptor leaks upon exec backup blocking new admin connections.
515401	SLBC-Dual mode: Slave chassis blade sending traffic logs.
516105	Daylight Saving Time is no longer in use in Azerbaijan.

User and Device

Bug ID	Description
500917	FSSO Collector Agent - Group change not synced back to FortiGate if last match to group-filter is removed.
519826	fnband crashing and ldap auth stopped working after upgrade.

VM

Bug ID	Description
305116	FOSVM unable to register with forticare.
498653	FortiOSVM stops passing traffic after failover.
512713	Connectivity loss between FGT-SVM and FGT-VMX cause license to become invalid after one hour.

Web Filter

Bug ID	Description
455193	Flow-based webfilter URL exempt not generating a UTM log.
499864	Web filter profile's proxy options to allow corporate Gmail accounts gets overlooked if "general interest" category is blocked under web filter.

WiFi Controller

Bug ID	Description
415981	WiFi Health Dashboard Enhancement: add AP name and AP group to Login Failures Information.
503106	Remote site client connected to the FAP14C ethernet port is randomly not able to reach the LAN client connected to the FortiGate.
503190	FAP info (apasn, apname, channel, radioband) missing from traffic logs.

Common Vulnerabilities and Exposures

Visit <https://fortiguard.com/psirt> for more information.

Bug ID	Description
510148	FortiOS 5.6.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">CVE-2018-15473

Known Issues

The following issues have been identified in version 5.6.7. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Application Control

Bug ID	Description
435951	Traffic keeps going through the <code>DENY</code> NGFW policy configured with URL category.
448247	Traffic-shaper in shaping policy does not work for specific application category like as P2P.

FortiGate-90E/91E

Bug ID	Description
393139	Software switch span doesn't work on this platform.

FortiGate 3815D

Bug ID	Description
385860	FG-3815D does not support 1GE SFP transceivers.

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.
357360	DHCP snooping may not work on IPv6.
369099	FortiSwitch authorizes successfully, but fails to pass traffic until you reboot FortiSwitch.
404399	FortiLink goes down when connecting to FortiSwitch 3.4.2 b192.

FortiView

Bug ID	Description
366627	FortiView Cloud Application may display incorrect drill down <i>File and Session</i> list in the <i>Applications View</i> .
368644	<i>Physical Topology: Physical Connection</i> of stacked FortiSwitch may be incorrect.

Bug ID	Description
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
408100	Log fields are not aligned with columns after drill down on FortiView and Log details.

GUI

Bug ID	Description
356174	FortiGuard updategrp read-write privilege admin cannot open FortiGuard page.
374844	Should show ipv6 address when set ipv6 mode to pppoe/dhcp on <i>GUI > Network > Interfaces</i> .
375383	If the policy includes the <i>wan-load-balance</i> interface, the policy list page may receive a javascript error when clicking the search box.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
445113	IPS engine 3.428 on Fortigate sometimes cannot detect Psiphon packets that iscan can detect.
451776	Admin GUI has limit of 10 characters for OTP.

HA

Bug ID	Description
481943	Green checkmarks indicating HA sync status on GUI only appear beside virtual cluster 1.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create webfilter logs.
503897	FortiGate-501E units generating logs only for five minutes after rebooting the unit, Then do not generate logs anymore.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
411368	In FortiView with FortiAnalyzer, the combined MAC address is displayed in the <i>Device</i> field.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.

System

Bug ID	Description
295292	If <code>private-data-encryption</code> is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
436580	PDQ_ISW_SSE drops at +/-100K CPS on FG-3700D with FOS 5.4 only.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
440411	Monitor NP6 IPsec engine status.
457096	FortiGate to FortiManager tunnel (FGFM) using the wrong source IP when multiple paths exist.
464873	RADIUS COA Disconnect-ACK message ignore RADIUS server <code>source-ip</code> setting.

VM

Bug ID	Description
441129	Certify FortiGate-VMX v5.6 with NSX v6.3 and vSphere v6.5.

Limitations

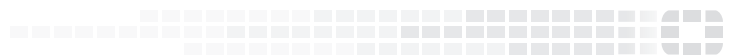
Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
 - XVA (recommended)
 - VHD
 - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.